A L E R T:

Following NSA document leak, EAC Issues Guidance and Recommendations

June 6, 2017

Consistent with the U.S. Election Assistance Commission's commitment to providing state and local election administrators with the information they need to ensure secure, accessible and accurate elections, the commission is issuing the following alert to state and local election officials:

According to credible news reports that surfaced yesterday, in the fall of 2016, a Russian-based hacker launched a phishing cyber-attack targeting more than 100 local U.S.-based election officials. The hacker sent these officials an email appearing to come from a private sector election services and equipment company. The goal was to trick officials into opening Microsoft Word documents carrying malware.

While phishing attacks are common across all sectors of our society and there is no evidence that this attack targeted voting machines involved in vote tallying of the 2016 Federal Election, this report provides a timely reminder that officials must remain vigilant about election system security.

The Federal Bureau of Investigation (FBI) and the Department of Homeland Security (DHS) are currently notifying the officials who were targeted by the attack and are coordinating the incident response.

As this story continues to unfold and law enforcement officials coordinate with those targeted by this phishing attach, the EAC is providing the following reminders, guidance and resources:

- Check email logs for emails from noreplyautomaticservice@gmail.com and vr.elections@gmail.com which were identified by the leaked NSA document as being the email addresses utilized by the attackers.

- Election officials should work with their IT officials and their Secretary of State's offices to routinely review systems and logs for possible malicious emails and other irregular activity.

- Election officials should monitor and actively seek security updates from state and national law enforcement and intelligence sources, including the DHS and FBI. EAC will provide these updates as we receive them.

- Follow election best practices by ensuring voting systems & corresponding EMS are NOT connected to the internet.

- Election officials should review security protocols with all staff and issue reminders to exercise caution when opening links and attachments, even those that appear to come from known senders.

- Visit the EAC's **"Election Security Preparedness"** page for information and checklists to guide security efforts, including:

    - Considerations for Implementing Voting Systems with COTS Products
    - Checklist - Securing Voter Registration Data
    - Checklist - Securing Election Night Reporting Systems
    - Ransomware and What to Do About It
    - Ten Things to Know About Selecting a Voting System
    - Ten Things to Know About Managing Aging Voting Systems
    - Cyber Incident Response Best Practices

- If you have found something of interest or have questions or concerns about this incident and its possible impact on your election jurisdiction, please contact the FBI cyber watch group at 1-855-292-3937 or cywatch@ic.fbi.gov. Election officials can also contact their local FBI field office. The EAC will follow up with additional information and resources as they become available. If the EAC can provide additional assistance, please do not hesitate to contact us.